IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:	Confirmation Number: 1614
Valiuddin Ali, *et al.*	Group Art Unit: 2137
Serial No.: 10/780,398	Examiner: Jeffrey L. Williams
Filed: February 17, 2004	Docket No.: 200314072-1

For: Computer Security System And Method

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Appeal Brief under 37 C.F.R. § 41.37 is submitted in support of the Notice of Appeal filed October 29, 2008, responding to the Final Office Action mailed August 12, 2008.

It is not believed that extensions of time or fees are required to consider this Appeal Brief. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. §1.136(a), and any fees required are hereby authorized to be charged to Deposit Account No. 08-2025.

I. Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. Related Appeals and Interferences

There are no known related appeals or interferences that will affect or be affected by a decision in this Appeal.

III. Status of Claims

Claims 1 – 46 stand finally rejected. No claims have been allowed. The final rejections of claims 1 – 46 are appealed.

IV. Status of Amendments

No amendments have been made or requested since the mailing of the Final Office Action and all amendments submitted prior to the Final Office action have been entered. The claims in the attached Claims Appendix IX (see below) reflect the present state of Appellants' claims.

V. Summary of Claimed Subject Matter

The claims are summarized below with reference numerals and references to the written description ("specification") and drawings. The subject matter described in the

following appears in the original disclosure at least where indicated, and may further appear in other places within the original disclosure.

Included are embodiments of a computer security system (page 2, line 20; and FIG. 1, element 10), that includes a processor (page 3, line 7; and FIG. 1, element 20) and a memory component (page 3, line 18; and FIG. 1, element 60) that stores a security module (page 3, line 26; and FIG. 1, element 70) adapted to control access to a secure computer resource (page 2, line 21) by a user via a client based on verification of a security credential (page 6, line 10; and FIG. 1, element 100) provided by the user and verification data (page 3, line 23; and FIG. 1, element 94) disposed on the client (page 2, line 21; and FIG. 1, element 12) and accessible by the security module (page 3, line 26; and FIG. 1, element 70), the security module adapted to enable the user to recover the security credential (page 6, line 10; and FIG. 1, element 100) from the client based on a response received from the user associated with the verification data.

Also included are embodiments of a computer security system (page 2, line 20; and FIG. 1, element 10) that includes means for controlling access to a secure computer resource associated with a client based on verification of a security credential (page 6, line 10; and FIG. 1, element 100) provided by a user of the client (page 3, line 7; FIG. 1, element 20; page 3, line 18; FIG. 1, element 60; page 3, line 26; and FIG. 1, element 70) means for accessing verification data disposed on the client to enable the user to recover the security credential (page 6, line 10; and FIG. 1, element 100) based on a response received from the user via the controlling means (page 3, line 7; FIG. 1, element 20; page 3, line 18; FIG. 1, element 60; page 3, line 23; and FIG. 94).

Also included are embodiments of a computer security method that includes receiving a request at a client to access a secure computer resource, a security credential (page 6, line 10; and FIG. 1, element 100) required from a user to access the secure computer resource (page 8, line 13); presenting verification data disposed on the

client to the user (page 9, line 16); and enabling the user to recover the security credential (page 6, line 10; and FIG. 1, element 100) from the client based on a response received from the user to the verification data (page 10, line 2).

Also included is a computer security system (page 2, line 20; and FIG. 1, element 10) that includes a processor (page 3, line 7; and FIG. 1, element 20) and a memory component (page 3, line 18; and FIG. 1, element 60) that stores a collection module adapted to receive and store verification data associated with a user on a client (page 5, line 21; and FIG. 1, element 80) and a recovery module adapted to enable the user to recover from the client a security credential (page 6, line 10; and FIG. 1, element 100) associated with accessing a secure computer resource via the client by verifying the user response to the verification data (page 6, line 19 and FIG. 1, element 82).

Also included is a computing device (page 2, line 20; and FIG. 1, element 10) that includes a processor (page 3, line 7; and FIG. 1, element 20) and a memory component (page 3, line 18; and FIG. 1, element 60) that stores a security module (page 3, line 26; and FIG. 1, element 70) disposed on the computing device and configured to control access to a secure computer resource associated with the computing device based on authentication of a security credential (page 6, line 10; and FIG. 1, element 100) and a recovery module (page 6, line 10; and FIG. 1, element 100) disposed on the computing device and configured to enable a user to retrieve the security credential from the computing device using verification data disposed on the computing device without accessing a resource external to the computer device.

VI. Grounds of Rejection to be Reviewed on Appeal

The following grounds of rejections are to be reviewed on appeal:

Claims 14 – 18 stand rejected under 35 U.S.C. §101 for allegedly being directed to non-statutory subject matter.

Claims 1 – 46 stand rejected under 35 U.S.C. §102 for allegedly being unpatentable over *Thompson* (European Patent Number 1,111,495).

VII. Arguments

Appellants respectfully submit that Appellants' claims 14 – 18 are patentable under 35 U.S.C. §101 and claims 1 – 46 are also patentable under 35 U.S.C. §102. Appellants respectfully request that the Board of Patent Appeals overturn the final rejection of those claims at least for the reasons discussed below.

A. The *Thompson* Reference

Thompson discloses "[w]hen the PC is booted, the security program executes first and prompts the user for a password… and compares it with the stored password. If the passwords do not match, boot is aborted and the PC is disabled… The encrypted password is also registered with a remote trusted certificate authority (TCA 150). To establish or change the password a communication connection is established from the PC to the TCA or storage device" (Abstract).

B. Rejections Under 35 U.S.C. §101

The Final Office Action indicates that claims 14 – 18 stand rejected under 35 U.S.C. §101 as allegedly being directed to non-statutory subject matter. The Final Office Action argues that "recitation of 'means for' does not necessarily result in a 'statutorily recognized claim." The Final Office Action continues, arguing that "[A]pplicant has shown within the [A]pplicant's specification that the recited means of claims 14 – 18 are implemented as software." Appellants disagree. More specifically, MPEP §2181, quoting the Court of Appeals for the Federal Circuit in In re Donaldson Co., 16 F.3d 1189, 29 USPQ2d 1845 (Fed. Cir. 1994), states "the 'broadest reasonable interpretation'

that an examiner may give means-plus-function language is that statutorily mandated in paragraph six. Accordingly, the PTO may not disregard the structure disclosed in the specification corresponding to such language when rendering a patentability determination" (emphasis added)

First, the present application clearly discloses structure for each of the claim elements of claims 14 – 18. More specifically, the as illustrated on page 3, among other places, the present application discloses a "client 12 [that] comprises a processor or central processing unit (CPU) 20; a memory 22 having an operating system 24…" (paragraph [0010]). Further, on page 8, the present application discloses that the "[s]ecurity module 70 may comprise software, hardware, or a combination of software and hardware" (paragraph [0012]).

As illustrated in the above cited passages of the written description, at least one embodiment for a "means for controlling" and a means for accessing" of claim 14, for example, includes a specific hardware component (*e.g.*, a processor and/or memory component) that is configured to implement the claimed function. Similarly, other embodiments may include a processor and/or a memory (and/or other components) that facilitate the recited function.

Second, the Examiner's statement is technologically incorrect. More specifically, as indicated above, the Examiner argues "[A]pplicant has shown within the [A]pplicant's specification that the recited means of claims 14 – 18 are implemented as software." This is an incorrect statement. As is clearly evident to one of ordinary skill in the art, software is merely a set of instructions that may be executed by computer hardware to perform one or more actions. Accordingly, software cannot perform any function of claims 14 – 18 without interaction with hardware. As a nonlimiting example, software (acting exclusively) cannot "access a secure computer resource" (claim 14) without

being executed on computer hardware. Consequently, the "means for" terminology that precedes the recited function must include hardware.

In its rejection, the Final Office Action neglects the disclosure of the corresponding structure in order to impermissibly limit the scope of claims 14 – 18 to only include software, contrary to 35 U.S.C. §112 ¶6 and MPEP §2181. Appellants explicitly utilize the "means for" language to invoke 35 U.S.C. §112 ¶6, to thereby capture structure disclosed in the specification. Accordingly, Appellants traverse this rejection and submit that claim 14 – 18 meet all the requirements of 35 U.S.C. §101.

C. Rejections Under 35 U.S.C. §102

1. Claim 1 is Allowable Over *Thompson*

The Final Office Action indicates that claim 1 stands rejected under 35 U.S.C. §102(b) as allegedly being anticipated by European Patent Number 1,111,495 ("*Thompson*"). Appellants respectfully traverse this rejection on the grounds that *Thompson* does not disclose, teach, or suggest all of the claimed elements. More specifically, claim 1 recites:

> A computer security system, comprising:
> a processor; and
> a memory component that stores:
> a security module adapted to control access to a secure computer resource by a user via a client based on verification of a security credential provided by the user; and
> verification data disposed on the client and accessible by the security module, the security module adapted to ***enable the user to recover the security credential from the client based on a response received from the user associated with the verification data***.
> ***(Emphasis added).***

Appellants respectfully submit that claim 1 is allowable over the cited art for at least the reason that *Thompson* fails to disclose, teach, or suggest a "computer security

system, comprising… a memory component that stores… verification data disposed on the client and accessible by the security module, the security module adapted to ***enable the user to recover the security credential from the client based on a response received from the user associated with the verification data***" as recited in claim 1. More specifically, the Final Office Action argues that *Thompson*, with regard to FIG. 4:

> herein disclosed is information disposed on the client which implements a recovery mechanism… for the purpose of examination, the examiner interprets "to recover the security credential from the client" in a manner consistent with the Applicant's specification. Specifically, the Applicant states in paragraph 15, "For example, as used herein, "recovering" security credential 100 includes enabling the user to independently reset security credential 100, and/or automatically having security credential 100 reset for the user by security module 70 without assistance from support personnel or an external computer resource.
> (OA page 3, line 13).

The Examiner referred to the specification to determine the proper scope of claim elements, but improperly analyzes the passage cited from the specification. More specifically, beginning on the first line paragraph [0015], the present application states "[v]erification data 94 comprises information associated with a query/response mechanism to enable the user of client 12 to independently recover a security credential 10 independent of a computer resource external to client 12" (emphasis added). As illustrated in this passage, the term "recover" is not limited to merely resetting a security credential. The term "recover," as used in the present application, is instead used to indicate an action that is utilized when the security credential is lost and/or is otherwise unavailable to a user.

Conversely, *Thompson* discloses receiving a password from a user (FIG. 4, block 404), determining whether the received password is valid (FIG. 4, block 408), and changing the password (FIG. 4, blocks 412, 414, 420). As illustrated in FIG. 4, the password of *Thompson* is known, and the user is merely changing the known password

to a new known password. Consequently, nothing in *Thompson* is "recovered" and thus, the Final Office Action has failed to establish a proper 35 U.S.C. §102(b) rejection. For at least these reasons, Appellants respectfully traverse this rejection, and submits that claim 1 is allowable in view of the cited art.

2. Claim 14 is Allowable Over *Thompson*

The Final Office Action indicates that claim 14 stands rejected under 35 U.S.C. §102(b) as allegedly being anticipated by European Patent Number 1,111,495 ("*Thompson*"). Appellants respectfully traverse this rejection on the grounds that *Thompson* does not disclose, teach, or suggest all of the claimed elements. More specifically, claim 14 recites:

> A computer security system, comprising:
> means for controlling access to a secure computer resource associated with a client based on verification of a security credential provided by a user of the client; and
> means for accessing verification data disposed on the client to ***enable the user to recover the security credential based on a response received from the user via the controlling means***.
> ***(Emphasis added).***

Appellants respectfully submit that claim 14 is allowable over the cited art for at least the reason that *Thompson* fails to disclose, teach, or suggest a "computer security system, comprising… means for accessing verification data disposed on the client to ***enable the user to recover the security credential based on a response received from the user via the controlling means***" as recited in claim 14. More specifically, the Final Office Action argues that *Thompson*, with regard to FIG. 4:

> herein disclosed is information disposed on the client which implements a recovery mechanism… for the purpose of examination, the examiner interprets "to recover the security credential from the client" in a manner consistent with the Applicant's specification. Specifically, the Applicant states in paragraph 15, "For example, as used herein, "recovering" security credential 100 includes

> enabling the user to independently reset security credential 100, and/or automatically having security credential 100 reset for the user by security module 70 without assistance from support personnel or an external computer resource.

(OA page 3, line 13).

The Examiner referred to the specification to determine the proper scope of claim elements, but improperly analyzes the passage cited from the specification. More specifically, beginning on the first line paragraph [0015], the present application states "[v]erification data 94 comprises information associated with a query/response mechanism to enable the user of client 12 to independently recover a security credential 10 independent of a computer resource external to client 12" (emphasis added). As illustrated in this passage, the term "recover" is not limited to merely resetting a security credential. The term "recover," as used in the present application, is instead used to indicate an action that is utilized when the security credential is lost and/or is otherwise unavailable to a user.

Conversely, *Thompson* discloses receiving a password from a user (FIG. 4, block 404), determining whether the received password is valid (FIG. 4, block 408), and changing the password (FIG. 4, blocks 412, 414, 420). As illustrated in FIG. 4, the password of *Thompson* is known, and the user is merely changing the known password to a new known password. Consequently, nothing in *Thompson* is "recovered" and thus, the Final Office Action has failed to establish a proper 35 U.S.C. §102(b) rejection. For at least these reasons, Appellants respectfully traverse this rejection, and submits that claim 14 is allowable in view of the cited art.

3. Claim 19 is Allowable Over *Thompson*

The Final Office Action indicates that claim 19 stands rejected under 35 U.S.C. §102(b) as allegedly being anticipated by European Patent Number 1,111,495 ("*Thompson*"). Appellants respectfully traverse this rejection on the grounds that

Thompson does not disclose, teach, or suggest all of the claimed elements. More specifically, claim 19 recites:

> A computer security method, comprising:
> receiving a request at a client to access a secure computer resource, a security credential required from a user to access the secure computer resource;
> presenting verification data disposed on the client to the user; and
> ***enabling the user to recover the security credential from the client based on a response received from the user to the verification data***.
> ***(Emphasis added).***

Appellants respectfully submit that claim 19 is allowable over the cited art for at least the reason that *Thompson* fails to disclose, teach, or suggest a "computer security method, comprising… ***enabling the user to recover the security credential from the client based on a response received from the user to the verification data***" as recited in claim 19. More specifically, the Final Office Action argues that *Thompson*, with regard to FIG. 4:

> herein disclosed is information disposed on the client which implements a recovery mechanism… for the purpose of examination, the examiner interprets "to recover the security credential from the client" in a manner consistent with the Applicant's specification. Specifically, the Applicant states in paragraph 15, "For example, as used herein, "recovering" security credential 100 includes enabling the user to independently reset security credential 100, and/or automatically having security credential 100 reset for the user by security module 70 without assistance from support personnel or an external computer resource.
> (OA page 3, line 13).

The Examiner referred to the specification to determine the proper scope of claim elements, but improperly analyzes the passage cited from the specification. More specifically, beginning on the first line paragraph [0015], the present application states "[v]erification data 94 comprises information <u>associated with a query/response mechanism to enable the user of client 12 to independently recover a security credential 10</u> independent of a computer resource external to client 12" (<u>emphasis added</u>). As

illustrated in this passage, the term "recover" is not limited to merely resetting a security credential. The term "recover," as used in the present application, is instead used to indicate an action that is utilized when the security credential is lost and/or is otherwise unavailable to a user.

Conversely, *Thompson* discloses receiving a password from a user (FIG. 4, block 404), determining whether the received password is valid (FIG. 4, block 408), and changing the password (FIG. 4, blocks 412, 414, 420). As illustrated in FIG. 4, the password of *Thompson* is known, and the user is merely changing the known password to a new known password. Consequently, nothing in *Thompson* is "recovered" and thus, the Final Office Action has failed to establish a proper 35 U.S.C. §102(b) rejection. For at least these reasons, Appellants respectfully traverse this rejection, and submits that claim 19 is allowable in view of the cited art.

4. Claim 31 is Allowable Over *Thompson*

The Final Office Action indicates that claim 31 stands rejected under 35 U.S.C. §102(b) as allegedly being anticipated by European Patent Number 1,111,495 ("*Thompson*"). Appellants respectfully traverse this rejection on the grounds that *Thompson* does not disclose, teach, or suggest all of the claimed elements. More specifically, claim 31 recites:

> A computer security system, comprising:
> a processor; and
> a memory component that stores:
> a collection module adapted to receive and store verification data associated with a user on a client; and
> a recovery module adapted to ***enable the user to recover from the client a security credential associated with accessing a secure computer resource via the client by verifying the user response to the verification data***.
> ***(Emphasis added).***

Appellants respectfully submit that claim 31 is allowable over the cited art for at least the reason that *Thompson* fails to disclose, teach, or suggest a "computer security system, comprising… a memory component that stores… a recovery module adapted to ***enable the user to recover from the client a security credential associated with accessing a secure computer resource via the client by verifying the user response to the verification data***" as recited in claim 31. More specifically, the Final Office Action argues that *Thompson*, with regard to FIG. 4:

> herein disclosed is information disposed on the client which implements a recovery mechanism… for the purpose of examination, the examiner interprets "to recover the security credential from the client" in a manner consistent with the Applicant's specification. Specifically, the Applicant states in paragraph 15, "For example, as used herein, "recovering" security credential 100 includes enabling the user to independently reset security credential 100, and/or automatically having security credential 100 reset for the user by security module 70 without assistance from support personnel or an external computer resource.

(OA page 3, line 13).

The Examiner referred to the specification to determine the proper scope of claim elements, but improperly analyzes the passage cited from the specification. More specifically, beginning on the first line paragraph [0015], the present application states "[v]erification data 94 comprises information associated with a query/response mechanism to enable the user of client 12 to independently recover a security credential 10 independent of a computer resource external to client 12" (emphasis added). As illustrated in this passage, the term "recover" is not limited to merely resetting a security credential. The term "recover," as used in the present application, is instead used to indicate an action that is utilized when the security credential is lost and/or is otherwise unavailable to a user.

Conversely, *Thompson* discloses receiving a password from a user (FIG. 4, block 404), determining whether the received password is valid (FIG. 4, block 408), and

changing the password (FIG. 4, blocks 412, 414, 420). As illustrated in FIG. 4, the password of *Thompson* is known, and the user is merely changing the known password to a new known password. Consequently, nothing in *Thompson* is "recovered" and thus, the Final Office Action has failed to establish a proper 35 U.S.C. §102(b) rejection. For at least these reasons, Appellants respectfully traverse this rejection, and submits that claim 31 is allowable in view of the cited art.

5. Claim 40 is Allowable Over *Thompson*

The Final Office Action indicates that claim 40 stands rejected under 35 U.S.C. §102(b) as allegedly being anticipated by European Patent Number 1,111,495 ("*Thompson*"). Appellants respectfully traverse this rejection on the grounds that *Thompson* does not disclose, teach, or suggest all of the claimed elements. More specifically, claim 40 recites:

> A computing device, comprising:
> a processor; and
> a memory component that stores:
> a security module disposed on the computing device and configured to control access to a secure computer resource associated with the computing device based on authentication of a security credential; and
> a recovery module disposed on the computing device and configured to ***enable a user to retrieve the security credential from the computing device using verification data disposed on the computing device without accessing a resource external to the computer device***.
> ***(Emphasis added).***

Appellants respectfully submit that claim 40 is allowable over the cited art for at least the reason that *Thompson* fails to disclose, teach, or suggest a "computing device, comprising… a memory component that stores… a recovery module disposed on the computing device and configured to ***enable a user to retrieve the security credential from the computing device using verification data disposed on the computing***

device without accessing a resource external to the computer device" as recited in claim 40. More specifically, the Final Office Action argues that *Thompson*, with regard to FIG. 4:

> herein disclosed is information disposed on the client which implements a recovery mechanism... for the purpose of examination, the examiner interprets "to recover the security credential from the client" in a manner consistent with the Applicant's specification. Specifically, the Applicant states in paragraph 15, "For example, as used herein, "recovering" security credential 100 includes enabling the user to independently reset security credential 100, and/or automatically having security credential 100 reset for the user by security module 70 without assistance from support personnel or an external computer resource.
> (OA page 3, line 13).

The Examiner referred to the specification to determine the proper scope of claim elements, but improperly analyzes the passage cited from the specification. More specifically, beginning on the first line paragraph [0015], the present application states "[v]erification data 94 comprises information associated with a query/response mechanism to enable the user of client 12 to independently recover a security credential 10 independent of a computer resource external to client 12" (emphasis added). As illustrated in this passage, the term "recover" is not limited to merely resetting a security credential. The term "recover," as used in the present application, is instead used to indicate an action that is utilized when the security credential is lost and/or is otherwise unavailable to a user.

Conversely, *Thompson* discloses receiving a password from a user (FIG. 4, block 404), determining whether the received password is valid (FIG. 4, block 408), and changing the password (FIG. 4, blocks 412, 414, 420). As illustrated in FIG. 4, the password of *Thompson* is known, and the user is merely changing the known password to a new known password. Consequently, nothing in *Thompson* is "recovered" and thus, the Final Office Action has failed to establish a proper 35 U.S.C. §102(b) rejection. For

at least these reasons, Appellants respectfully traverse this rejection, and submits that claim 40 is allowable in view of the cited art.

6. Claims 2 – 13, 15 – 18, 20 – 30, 32 – 39, and 41 – 46 are Allowable Over *Thompson*

The Final Office Action indicates that claims 2 – 13, 15 – 18, 20 – 30, 32 – 39, and 41 – 46 stand rejected under 35 U.S.C. §102(b) as allegedly being anticipated by European Patent Number 1,111,495 ("*Thompson*"). Appellants respectfully traverse this rejection on the grounds that *Thompson* does not disclose, teach, or suggest all of the claimed elements. More specifically, dependent claims 2 – 13 are believed to be allowable for at least the reason that these claims depend from and include the elements of allowable independent claim 1. Dependent claims 15 – 18 are believed to be allowable for at least the reason that these claims depend from and include the elements of allowable independent claim 14. Dependent claims 20 – 30 are believed to be allowable for at least the reason that these claims depend from and include the elements of allowable independent claim 19. Dependent claims 32 – 39 are believed to be allowable for at least the reason that these claims depend from and include the elements of allowable independent claim 31. Dependent claims 41 – 46 are believed to be allowable for at least the reason that these claims depend from and include the elements of allowable independent claim 40. *In re Fine*, *Minnesota Mining and Mfg.Co. v. Chemque, Inc.*, 303 F.3d 1294, 1299 (Fed. Cir. 2002).

VIII. Conclusion

In summary, it is Appellants' position that Appellants' claims are patentable over the applied cited art references and that the rejection of these claims should be withdrawn. Appellants therefore respectfully request that the Board of Appeals overturn the Examiner's rejection and allow Appellants' pending claims.

Respectfully submitted,

By: /afb/
Anthony F. Bonner, Jr.
Registration No. 55,012

Claims Appendix under 37 C.F.R. § 41.37(c)(1)(viii)

The following are the claims that are involved in this Appeal.

1. A computer security system, comprising:

a processor; and

a memory component that stores:

a security module adapted to control access to a secure computer resource by a user via a client based on verification of a security credential provided by the user; and

verification data disposed on the client and accessible by the security module, the security module adapted to enable the user to recover the security credential from the client based on a response received from the user associated with the verification data.

2. The system of Claim 1, wherein the security module is adapted to enable the user to reset the security credential based on the response.

3. The system of Claim 1, wherein the security module is adapted to generate a query to present to the user based on the verification data.

4. The system of Claim 1, wherein the security module is adapted to control booting of the client based on the response.

5. The system of Claim 1, wherein the security module is adapted to initiate a collection module to acquire the verification data from the user.

6. The system of Claim 1, wherein the security module is adapted to encrypt the security credential based on the verification data.

7. The system of Claim 1, wherein the security module is adapted to decrypt an encrypted security credential based on the response.

8. The system of Claim 1, wherein the security module is disposed in a basic input/output system (BIOS).

9. The system of Claim 1, wherein the security module is adapted to control access to a secure communications network.

10. The system of Claim 1, wherein the security module is adapted to control access to a computer network resource.

11. The system of Claim 1, wherein the security module is adapted to enable the user to retrieve the security credential based on the response.

12. The system of Claim 1, wherein the security module is adapted to automatically reset the security credential based on the response.

13. the system of Claim 1, wherein the security module is disposed on the client.

14. A computer security system, comprising:

means for controlling access to a secure computer resource associated with a client based on verification of a security credential provided by a user of the client; and

means for accessing verification data disposed on the client to enable the user to recover the security credential based on a response received from the user via the controlling means.

15. The system of Claim 14, wherein the means for accessing comprises means for generating a query presentable to the user.

16. The system of Claim 14, wherein the controlling means comprises means for controlling booting of the client based on the response.

17. The system of Claim 14, further comprising means for initiating a collection module for acquiring verification data from the user.

18. The system of Claim 14, further comprising means for automatically resetting the security credential based on the response.

19. A computer security method, comprising:

receiving a request at a client to access a secure computer resource, a security credential required from a user to access the secure computer resource;

presenting verification data disposed on the client to the user; and

enabling the user to recover the security credential from the client based on a response received from the user to the verification data.

20. The method of Claim 19, further comprising initiating booting of the client based on the response.

21. The method of Claim 19, wherein presenting the verification data comprises generating a query to present to the user for recovery of the security credential.

22. The method of Claim 19, wherein enabling the user to recover the security credential comprises enabling the user to reset the security credential based on the response.

23. The method of Claim 19, further comprising initiating a collection module to acquire the verification data from the user.

24. The method of Claim 19, further comprising encrypting the security credential based on the response received from the user to the verification data.

25. The method of Claim 19, further comprising decrypting an encrypted security credential based on the response received from the user to the verification data.

26. The method of Claim 19, further comprising receiving the response to a query presented to the user for recovery of the security credential.

27. The method of Claim 19, further comprising accessing a secure computer communications network based on the response.

28. The method of Claim 19, further comprising accessing a secure computer network resource based on the response.

29. The method of Claim 19, wherein enabling the user to recover the security credential comprises enabling the user to retrieve the security credential based on the response.

30. The method of Claim 19, wherein enabling the user to recover the security credential comprises automatically resetting the security credential for the user based on the response.

31. A computer security system, comprising:

a processor; and

a memory component that stores:

a collection module adapted to receive and store verification data associated with a user on a client; and

a recovery module adapted to enable the user to recover from the client a security credential associated with accessing a secure computer resource via the client by verifying the user response to the verification data.

32. The system of Claim 31, wherein the recovery module is adapted to generate a query presentable to the user based on the verification data.

33. The system of Claim 31, wherein the recovery module is adapted to enable the user to reset the security credential.

34. The system of Claim 31, wherein the recovery module is disposed within a basic input/output system (BIOS).

35. The system of Claim 31, further comprising an encryption/decryption module adapted to encrypt the security credential using the verification data.

36. The system of Claim 31, further comprising an encryption/decryption module adapted to decrypt the security credential based on the response.

37. The system of Claim 31, wherein the recovery module is adapted to enable the user to retrieve the security credential.

38. The system of Claim 31, wherein the recovery module is adapted to automatically reset the security credential for the user based on the user response.

39. The system of Claim 31, wherein the recovery module is disposed on the client.

40. A computing device, comprising:

a processor; and

a memory component that stores:

a security module disposed on the computing device and configured to control access to a secure computer resource associated with the computing device based on authentication of a security credential; and

a recovery module disposed on the computing device and configured to enable a user to retrieve the security credential from the computing device using

verification data disposed on the computing device without accessing a resource external to the computer device.

41. The device of Claim 40, wherein the recovery module enables a user to independently retrieve the security credential.

42. The device of Claim 40, wherein the recovery module enables a user to independently reset the security credential.

43. The device of Claim 40, wherein the recovery module automatically resets the security credential for the user in response to retrieving the security credential.

44. The device of Claim 40, wherein the recovery module is configured to retrieve the security credential based on a response received from the user associated with the verification data.

45. The device of Claim 40, wherein the verification data comprises data associated with a query and response mechanism.

46. The device of Claim 40, wherein the security module is disposed in a basic input/output system (BIOS).

Evidence Appendix under 37 C.F.R. § 41.37(c)(1)(ix)

(none)

Related Proceedings Appendix under 37 C.F.R. § 41.37(c)(1)(x)

(none)